FIG 1

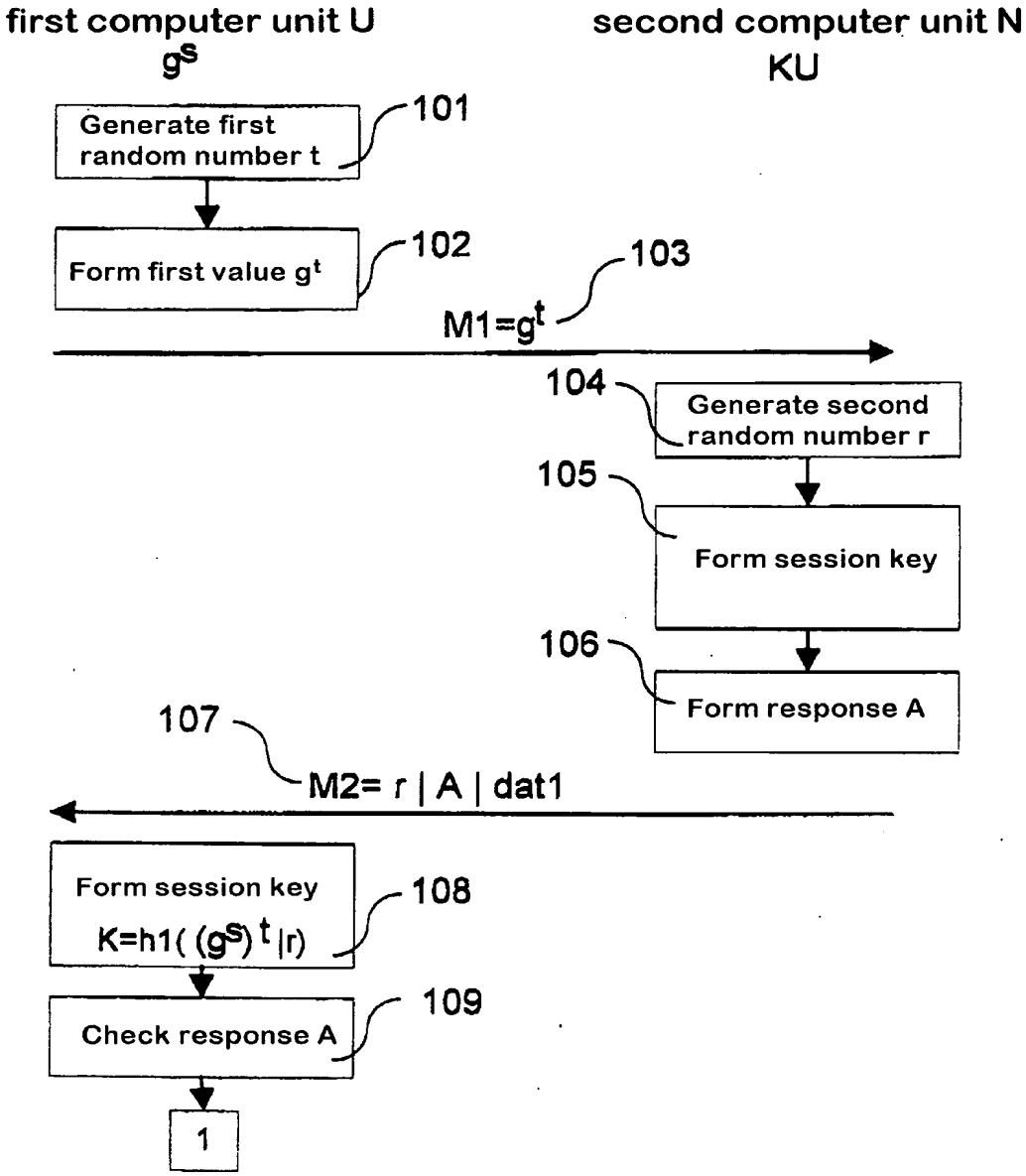

first computer unit U
g^s
second computer unit N
KU
Generate first random number t
101
Form first value g^t
102
103
$M1=g^t$
104
Generate second random number r
105
Form session key
106
Form response A
107
M2= r | A | dat1
Form session key
$K=h1((g^s)^t|r)$
108
Check response A
109
1

FIG 1

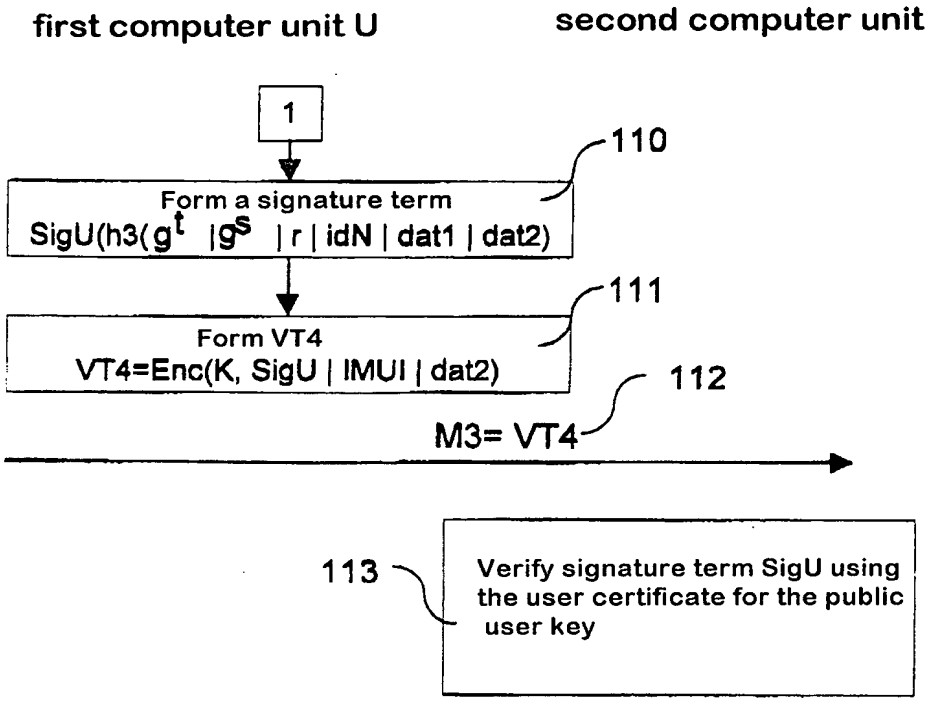

first computer unit U
second computer unit N
1
110
Form a signature term
SigU(h3(g^t |g^s | r | idN | dat1 | dat2)
111
Form VT4
VT4=Enc(K, SigU | IMUI | dat2)
112
M3= VT4
113
Verify signature term SigU using the user certificate for the public user key

FIG 2

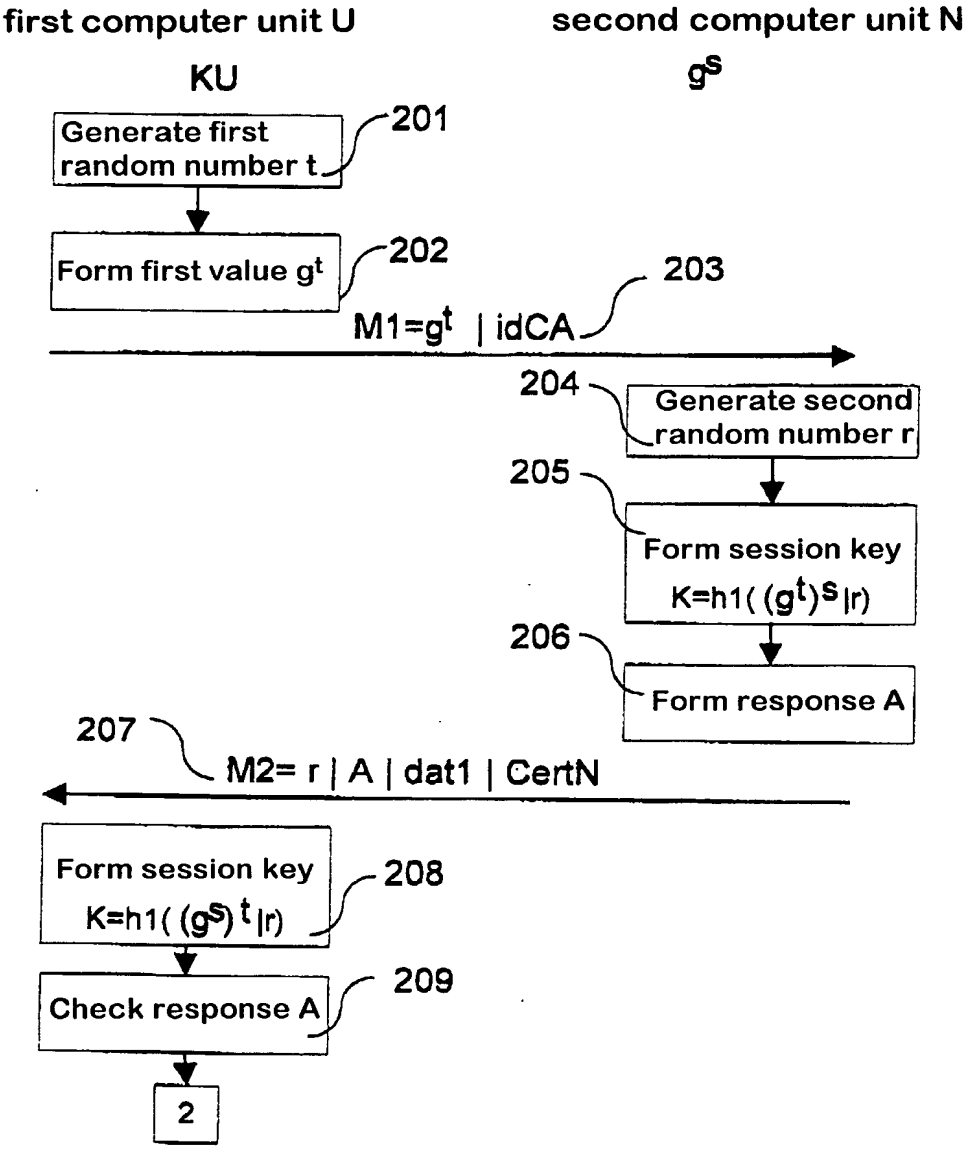

first computer unit U
KU
second computer unit N
g^s
Generate first random number t
201
Form first value g^t
202
203
$M1=g^t \mid idCA$
204
Generate second random number r
205
Form session key
$K=h1((g^t)^s \mid r)$
206
Form response A
207
$M2= r \mid A \mid dat1 \mid CertN$
Form session key
$K=h1((g^s)^t \mid r)$
208
Check response A
209
2

FIG 2

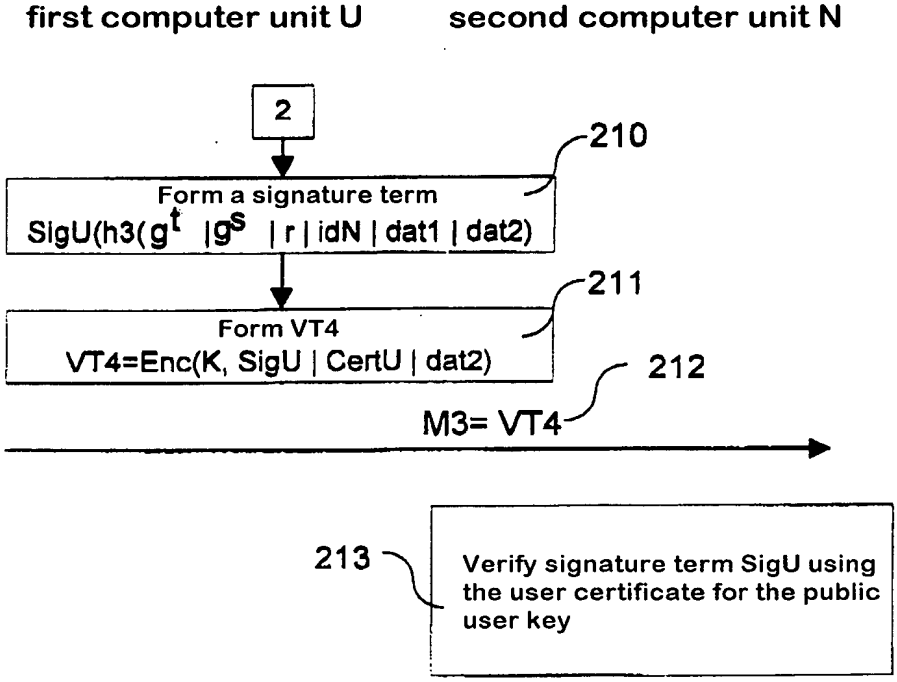

first computer unit U
second computer unit N
2
210
Form a signature term
SigU(h3(g^t |g^s | r | idN | dat1 | dat2)
211
Form VT4
VT4=Enc(K, SigU | CertU | dat2)
212
M3= VT4
213
Verify signature term SigU using the user certificate for the public user key

FIG 3

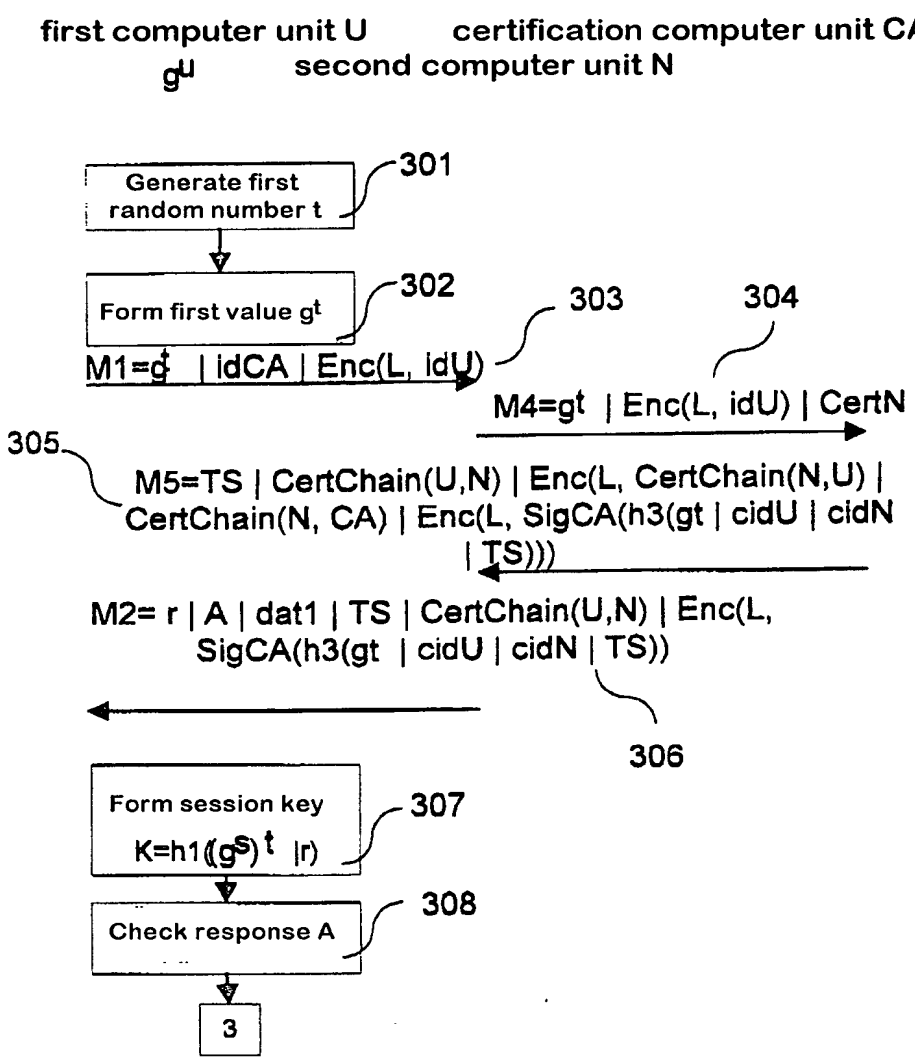
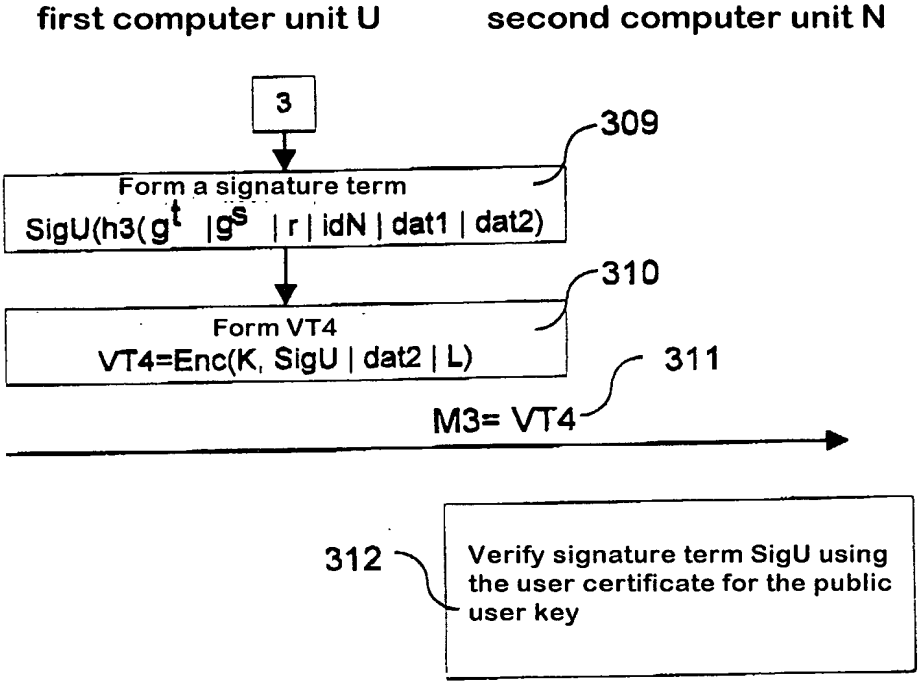

first computer unit U
certification computer unit CA
g^u
second computer unit N
Generate first random number t
301
Form first value g^t
302
303
304
M1=g^t | idCA | Enc(L, idU)
M4=g^t | Enc(L, idU) | CertN
305
M5=TS | CertChain(U,N) | Enc(L, CertChain(N,U) | CertChain(N, CA) | Enc(L, SigCA(h3(gt | cidU | cidN | TS)))
M2= r | A | dat1 | TS | CertChain(U,N) | Enc(L, SigCA(h3(gt | cidU | cidN | TS))
306
Form session key
K=h1((g^s)^t |r)
307
Check response A
308
3

FIG 3


first computer unit U
second computer unit N
3
309
Form a signature term
SigU(h3(g^t |g^s | r | idN | dat1 | dat2)
310
Form VT4
VT4=Enc(K, SigU | dat2 | L)
311
M3= VT4
312
Verify signature term SigU using the user certificate for the public user key